Method for Developing Security Procedures in a DRE Environment

Dana DeBeauvoir, Travis County Clerk

As November 2004 approached, everyone seemed to have one issue on his or her mind. From newspapers to television comedy to conversations in coffee houses, the Presidential election was the hot topic. But, this election year was different from four years ago. The 2000 Florida controversy, the resulting large-scale implementation of electronic voting, the strong memories of the 9/11 tragedy, and the polarized opinions of the country had culminated into a general anxiety not only about who was going to win but whether our election process could be disrupted and the results trusted.

In Travis County, Texas, we not only fielded questions of concern from citizens, political parties, candidates, and media organizations; we had our own uneasy feelings, feelings that turned from worry to conviction. We were going to do whatever it took to make sure our election was protected and that the public could trust that it was safe, fair, and accurate, no matter what happened here or anywhere in the world. That was an admirable, lofty goal, but how do you implement stubborn determination?

Believe it or not, we laid an egg. Our first inspiration for the egg came from our association with the legal community and their use of the rules of evidence. According to Article I of the Federal Rules of Evidence, "these rules shall be construed to secure fairness in administration, elimination of unjustifiable expense and delay, and promotion of growth and development of the law of evidence to the end that the truth may be ascertained and proceedings justly determined."

Make no mistake, we are not attorneys, but when we saw their standards for rules of evidence, we thought they were on to something. To give support and integrity to evidence, you need to make sure you have: something physical (reports, audit logs, etc.), recorded details about persons who were involved in creating or collecting the evidence (times, dates, names, signatures, etc.), and secure storage so that evidence cannot be tampered with (areas with limited access). We decided to adapt these standards to our election processes.

The second part of this idea came from our computer staff and their obsession with developing risk analyses. So, we broke down the election process into categories and began to brainstorm about the possible minor or catastrophic events that could happen in each area. (Coming up with scenarios of horrible events is easier than you think thanks not only to real life news stories, but our exposure to the creative minds of television and movie scriptwriters.)

As ideas poured out, the rule quickly became that generalities had to be broken down to tangible events. For example, to say, "someone could tamper with the DRE system" had to be followed up with ideas of specifically how someone would go about doing such a deed. Therefore, what we ended up with was a tool that provided perspective, replaced emotion with facts, and guided us to a detailed plan of action.

If you look at the attachments, you will see the evolution of our egg and examples of how we combined all of our ideas into a method of mitigating risks and providing verifiable checks and audits that election procedures were properly followed.

The result of our egg analysis was not only a new way of thinking for us, but also a plan and checklist for what needed to be done for the 2004 election and for all future elections. The process led us to reinforce and fine-tune many of our existing practices and to develop new initiatives. Listed below are some examples of new, continued, or enhanced practices that increase a secure election environment and promote public trust. Examples of these items are provided in the attachments, and since we are particularly proud of the work we did to increase security by using hash code and parallel testing, we have included more detail on these practices.

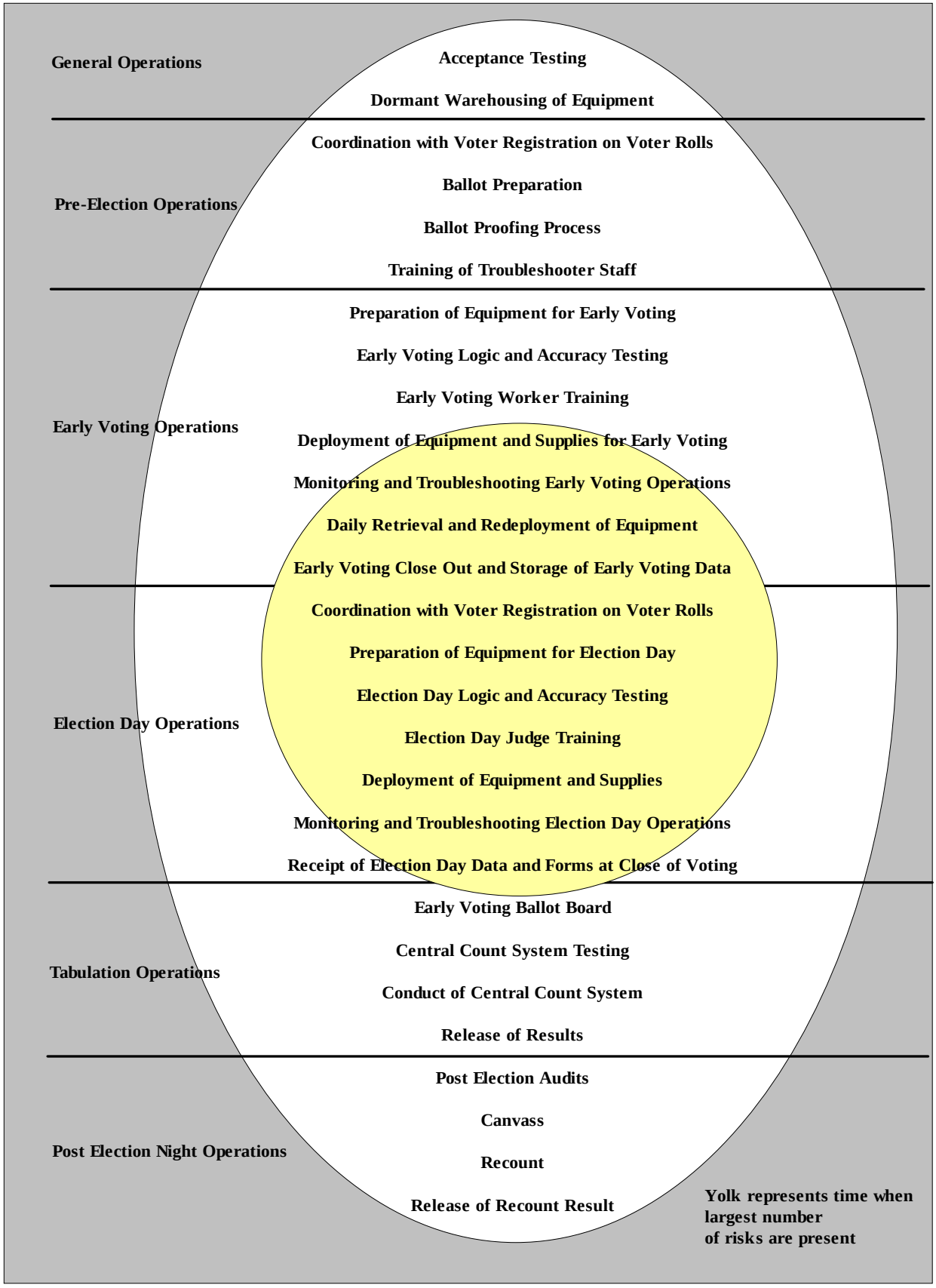
New, Enhanced, or Continued Security Practices

- Provide public invitation to attend all programming and testing activities
- Maintain written procedures and initialed tracking sheets
- Maintain independence from vendors
- Recruit, screen, and train skilled and trusted employees
- Coordinate emergency management plans with other relevant agencies
- Use Sheriff and Constable Officers to secure early voting electronic ballot boxes
- Improve security for the building where election activities occur
- Implement employee procedures that lower risk
- Conduct extensive pre-purchase testing of new equipment or software
- Provide continuous functionality testing of equipment
- Conduct Hash Code Testing on software
- Perform High Volume Testing of ballot programming
- Perform Parallel Testing
- Conduct Early Voting and Election Day audits by matching counts of voters by location as reported by the electronic voting system to the number of names on signature rosters
- Conduct post-election verification using the three redundant electronic sources, paper results printed from the electronic ballot boxes, and precinct-by-precinct election results

(When reviewing these practices, it may be helpful to understand that in Texas, a County cannot use a voting system unless the Texas Secretary of State has certified it. To date, no system allowing voter-verifiable paper ballots has been authorized, and therefore, could not be considered for use in the 2004 Presidential Election.)

Finally, about that egg concept... after you have read this, you may ask why we went with an egg shape instead of a rectangle or a circle. Truth be told, it started because the County Clerk's first drawing of an oval was less than perfect and resembled an egg. However, we capitalized on that idea. After all, we were birthing a new idea. Second, an egg has a hard shell wrapped around a permeable membrane. The shell ultimately served as a perfect metaphor and guide for determining the security levels needed for different groups (general public, candidates, law enforcement, etc.), and the membrane represented how information would flow back and forth through the process. Finally, the egg became a symbol for us. It is something with immeasurable value; something that must be given great love, care, and protection; and something that represents elections as the beginning and nucleus for a living democracy.

Egg Concept for Defining and Mitigating Security Risks in a DRE Environment



General Operations

Acceptance Testing

Dormant Warehousing of Equipment

Pre-Election Operations

Ballot Preparation

Coordination with Vote Registrar on Rolls

Ballot Proofing Process

Training of Troubleshooter Staff

Early Voting (EV) Operations

Preparation of Equipment

Logic and Accuracy Testing

Worker Training

Deployment of Equipment and Supplies

Monitoring and Troubleshooting

Daily Retrieval and Redeployment of Equipment

Close Out and Storage of EV Data

Election Day Operations

Coordination with Vote Registrar on Rolls

Preparation of Equipment for Election Day

Logic and Accuracy Testing

Election Day Judge Training

Deployment of Equipment and Supplies

Monitoring & Troubleshooting Operations

Receipt of Election Day Data and Forms at Close of Voting

Tabulation Operations

Early Voting Ballot Board

Central Count System Testing

Conduct of Central Count System

Release of Results

Post Election Night Operations

Post Election Audits

Canvass

Recount

Release of Recount Results

A Few Examples of Risk Assessments and Strategies Devised to Reduce Risks

Independently Test Voting System Products Before Purchase and Use
Risk: Equipment or software is inferior or subject to vendor manipulation.
Practice: Perform hands-on mock trial of equipment or software with vendor present only to answer questions. Produce and audit all available reports. For important demonstrations (such as purchase of new voting system) include diverse group of outside parties to view and participate in testing. Have sign in sheet of viewers and request written evaluations and comments from participants.

Prevent Physical Damage to Electronic Voting Equipment
Risk: Fire in warehouse and activation of sprinkler system damages DRE equipment.
Practice: Cover equipment carts with plastic covers to prevent water damage.

Physically Secure Ballot Programming Computer
Risk: Unauthorized user tampers with ballot programming computer.
Practice: Ballot programming and tabulation computer is kept in room with a motion detector, surveillance camera, and pass code lock. Five employees issued pass code. Ballot software is protected by a series of passwords that are issued only to five employees. Use of this computer is only done when two or more authorized employees/watchers are present.

Protect Early Voting Electronic Ballot Box
Risk: Theft or tampering of early voting ballot box after hours at early voting locations.
Practice: Every night during Early Voting, the electronic ballot boxes are picked up at the polling locations by law enforcement officers. Overnight the boxes are locked in a secured room with a surveillance camera. During the Presidential Election, we were even more vigilant and had law enforcement officers stationed outside the room during the evenings. Each morning, law enforcement transported the boxes back out to the early voting locations.

Promote Openness of the Tabulation Process
Risk: Perception that unethical practices are occurring behind the scenes on Election Night.
Practice: On Election Day and Night, poll watchers, party officials, and oversight committee members are encouraged to closely observe all election night activities. All tabulation activities are performed in a room with windows so that all members of the general public and the media can view the proceedings.

Use of Parallel Testing to Detect Presence of "Time Bomb" Software Codes

(Abbreviated version of our procedures as used with Hart Intercivic E-Slate System)

Risk: Introduction of malicious software program written so that it is activated during the actual election process and therefore goes undetected in pre-election testing.

Practice: Perform parallel testing during Early Voting and Election Day to ensure that no such program is being activated. Randomly pull out equipment slated for polling location just before it is to be sent out. Perform testing in ELECTION mode so that it mirrors the election cycle of opening polls, casting ballots, and closing polls. Conduct test in a controlled environment under video surveillance. Encourage public viewing of test.

A. Parallel Test Spreadsheet

1. Create a spreadsheet using the Logic and Accuracy spreadsheet as a template.
2. Randomly enter votes for each precinct in no particular pattern (so software will not identify if it as a test).
3. Include enough ballots to ensure at least two ballots are cast per hour per day.

B. Paper Ballots

1. Using the Parallel Test spreadsheet, mark all paper ballots according to spreadsheet.
2. Double check ballots where marked correctly to ensure 100% accuracy.
3. Make a stack of ballots for each day of Early Voting and one stack for Election Day.

C. Polling Location Equipment

1. Randomly select a polling location during the day of delivery of equipment.
2. Replace removed equipment with extra equipment.
3. Place equipment in secured area and clearly mark as PARALLEL TEST EQUIPMENT.

D. Ballot Box Preparation

1. Gather 2 Ballot boxes with red seals. (one for Early Voting and one for Election Day)
2. Lock and seal the boxes. Record the seal numbers. Seals are not broken until the end of each test period.

E. Secured Area

1. Setup all parallel test equipment where all actions are visibly recorded by video surveillance.
2. Tag area with PARALLEL TEST – AUTHORIZED PERSONNEL ONLY signs.

F. Casting Votes

1. Use ballots designated for the specified day and corresponding parallel test.
2. Retrieve an access code for the first ballot and begin voting ballot one e-Slate as marked on paper ballot.
3. Once ballot has been cast print your initials, date, and time on the top right hand corner of the paper ballot.
4. Then print your initials, date, and time on the parallel test spreadsheet.
5. Staple access code to paper ballot on top left hand corner.
6. Insert paper ballot into ballot box.
7. Two ballots per hour per day should be voted.

G. Tabulation of results

1. Once the parallel test is completed, all materials should be placed in the BOSS room.
2. Tabulation of results will occur after the Official Elections results have been finalized.
3. Create a database in TALLY named PARALLEL TEST - "Name of election".
4. Insert MBB cards from parallel test equipment.
5. Tabulate results.
6. Print Cumulative reports.

H. Backup equipment (SERVO)

1. Using SERVO, create an event using the same naming convention in TALLY.
2. Backup all parallel test equipment to this event.
3. Print out "Devices backed up report".
4. Compare totals between TALLY, SERVO, and the parallel test spreadsheet. Totals should match identically.

Use of Hash Code Testing to Detect Modification of Software
(Abbreviated version of our procedures as used with Hart Intercivic E-Slate System)

Risk: Modification of software by vendor, employee, or outsider.

Practice: Use Hash Code testing to verify that software files installed on computers are the same as the software files qualified by an Independent Testing Authority and certified by the Secretary of State. Hash Code is a digital algorithm signature of a variable-sized amount of text that is converted into a fixed-sized output that can be used to determine if two objects are equal. Testing must be performed before and after the software is used in an election.

A. Create Hash Code Spreadsheet

1. Access NIST website to obtain hash types and file names. (www.nsrl.nist.gov/votedata.html)
2. Download zip format file from website.
3. Open file CompleteNSRLfile.txt in Excel and follow steps in Excel wizard when opening the text document.
4. Sort by Product Code, then File Name. Delete rows NOT for Code 9031. (9031 is for our e-Slate system.)
5. Save file.

B. Install Hash Master Software

1. Verify that each station has the Hash Master software installed. If not, use the setup.exe file on installation CD.
2. Follow instructions in the software wizard to complete installation of Hash Master.

C. Execute the Hash Code function (from Readme.txt)

1. To calculate and display the hash of a file:
    a. From the File menu, select "Select Algorithm." The "Configure Hash Options" window appears.
    b. Select the hash algorithm to be used (Travis County uses MD5 or SHA-1).
    c. Click "Save." The hash algorithm selected displays in the Hash Master window.
    d. From the File menu, select Process Files. The "Select one or more files to process" window appears.
    e. In the Look In field, find the directory that contains the file(s) to be processed. Complete one group of files per software at a time. Refer to the Hash Code spreadsheet to determine file paths for each software type.
    f. Select the file(s) to be processed.
    g. Click the Open button. The "Select one or more files to process" window closes. The path to the last file selected and its hash value appear in the Hash Master window.
        1. To copy the hash to the Clipboard: From the Edit menu, select Copy Hash to Clipboard. —OR— While in the Hash Master window, hold down the Ctrl key and press C.
        2. To view the File Hash Report for the file(s) just processed: From the Report menu, select View Report. The "Hash Report" window appears showing the File Hash Report. The File Hash Report contains the path and hash value for each file processed with the Process Files command.
        3. To print the File Hash Report for the file(s) just processed: From the Report menu, select Print Report. —OR—View the report, then click the Print tool icon at the top of the Hash Report window.
        4. To save the File Hash Report as PDF for the file (s) just processed: From the Report menu, select Save report as PDF. The Save report as PDF window appears showing the file directory. Indicated the file name and location where you want to save. Click the save button.
        5. To run the Third Party Hash for the last file just processed: Do not change the hash algorithm that was in effect when you processed the file. From the File menu, select Third Party. A command prompt window appears. Wait until the third-party hash utility finishes.
2. After completing one group of files for a specific software and hash type, exist Hash Master and repeat the process for all files for each software and Hash Type from the beginning.

D. Compare Hash Code files

1. Generate a paper report from Hash Master for each computer, hash type, and group of files. Staple each report to the Hash Code spreadsheet that corresponds to each group of files.
2. Label each report to identify which computer it was generated from. (i.e. BOSS computer)
3. Compare Hash Code files generated from Hash Master to files located on the Hash Code Spreadsheet. All files should be accounted for and match identically.